

Технически Университет - София

Курсова Работа

По Основи на Мрежовите Технологии (ОМТ)

На тема:

Ethernet технология.

Методи и средства за анализ на работата на Ethernet.

Мрежов дизайн за най-добра производителност.

Разработил:

Лъчезар Христов Спириев

Специалност: Телекомуникации

Факултет: Телекомуникации

Ф-н: 111221054

Група: 54

Проверил:

1 Въведение в тематика: **Ethernet технология**

Ethernet е вид комуникационен протокол, създаден в Xerox PARC през 1973 г., който свързва компютри в мрежа чрез кабелна връзка (коаксиална, оптична или усукана двойка). Това е широко използван LAN протокол. Той свързва компютри в рамките на локалната мрежа (LAN) и широкообхватната мрежа (WAN).

Ethernet предлага прост потребителски интерфейс, който помага за лесно свързване на различни устройства, като суичове, рутери и компютри. Локална мрежа може да бъде създадена с помощта на един рутер и няколко Ethernet кабела, които позволяват комуникация между всички свързани устройства. Ethernet описва как мрежовите устройства форматират и предават данни, така че други устройства в същата LAN или кампусна мрежа да могат да разпознават, получават и обработват информацията.

Ethernet кабелът е физическото окабеляване, по което се движат данните. Ако две или повече свързани устройства в споделена мрежа се опитат да предадат пакети данни едновременно, възниква сблъсък на пакети. Импулсите от електричество или фотони, които съставляват пакет, се припокриват, когато се изпращат едновременно по споделен меден или оптичен кабел. Ethernet е проектиран да реши проблема със сблъсъка на пакети.

1.1 Запознаване с методите и средства за анализ на работата на Ethernet.

Има няколко метода за анализ на Ethernet, в зависимост от целите на анализа и инструментите, които се използват. Това са примери за някои методи за анализ:

Улавяне на пакети (Packet Capture): Това включва улавяне на всички пакети в мрежовия сегмент с помощта на инструмент като Wireshark™. Този метод позволява подробен анализ на всеки пакет, включително заглавията, данните и информацията за времето.

Анализ на протокола: Това включва анализ на трафика в мрежовия сегмент, за да се идентифицират използваните протоколи и начина, по който се използват. Този метод може да помогне за идентифициране на проблеми с мрежата и уязвимости за сигурност.

Анализ на трафика: Това включва анализ на трафиковите шаблони в мрежовия сегмент, за да се идентифицират тенденции, аномалии и потенциални проблеми. Този метод може да помогне за идентифициране на шаблони на злоупотреба, определяне на претоварени или недостатъчно използвани мрежови сегменти и оптимизиране на производителността на мрежата.

Анализ на производителността: Това включва анализ на мрежовите метрики за производителност, като закъснение, пропускателна способност и загуба на пакети, за да се идентифицират проблеми с производителността и да се оптимизира производителността на мрежата. Този метод може да бъде

използван за идентифициране на затруднени места, оптимизиране на мрежовите конфигурации и подобряване на потребителския опит.

Анализ на сигурността: Това включва анализ на мрежовия трафик, за да се идентифицират уязвимости за сигурност и потенциални атаки. Този метод може да бъде използван за идентифициране на шаблони на злоупотреба, определяне на компрометирани хостове и предотвратяване или облекчаване на атаки.

1.2 Въведение в мрежовият дизайн на Ethernet:

Ethernet мрежите могат да бъдат проектирани по различни начини, за да отговарят на специфичните нужди на организацията, в зависимост от фактори като броя на устройствата в мрежата, количеството генериран трафик и други.

Една от честите мрежови конфигурации на Ethernet е топология звезда, при която всички устройства се свързват към централен суич или хъб. Това позволява лесно управление на мрежата, тъй като устройства могат да бъдат добавяни или премахвани без да нарушават цялата мрежа. Друг вид мрежов дизайн е мрежова топология "мрежа", при която всяко устройство е свързано с множество други устройства във формата на паяжинеста структура. Този дизайн осигурява защита от смущения, тъй като трафикът може да бъде пренасочен, ако един от линковете не работи.

Освен физическия дизайн на мрежата, мрежите на Ethernet могат да бъдат проектирани с различни мрежови протоколи и технологии, като VLAN, Quality of Service (QoS) и Link Aggregation Control Protocol (LACP). VLAN-ите позволяват на мрежовите администратори да разделят трафика на

мрежата на логически сегменти, докато QoS придава приоритет на определени видове трафик над други. LACP позволява свързването на множество физически връзки в една логическа връзка, което осигурява редундантност и увеличава пропускателната способност.

2 По-дълбоко разглеждане на Методите и средствата за анализ на Ethernet.

2.1 Улавяне на пакети (Packet Capture)

Мрежите прехвърлят информация от един компютър на друг под формата на пакети.

Най-често срещаните са пакети на интернет протокол версия 4 (IPv4), пренасяни през Ethernet рамки. IPv4 пакетите включват заглавие и полезен товар. Заглавието включва важна информация за маршрутизиране на пакета в интернет, включително адрес на източника и местоназначението, а полезният товар съдържа действителните данни, които се предават. Много ценна информация може да бъде получена чрез декодиране на пакети като:

- Къде се изпращат тези мрежови пакети?
- Кой ги изпрати?
- Какво се изпраща вътре в пакетите?

Улавянето на мрежови пакети е актът на записване на пакети, които преминават през компютърна мрежа, включително всеки хедър на пакет и полезен товар. След като пакетите бъдат уловени, ИТ персоналът може да

види заглавието и полезния товар на всеки уловен пакет с помощта на GUI базиран преглед на декодиране. Файловете за улавяне на пакети могат да бъдат записани във файл с общ формат като pcap, pcapng или erf.

Улавянето на пакети се използва за разследване на заплахи за сигурността или търсене на основната причина за проблеми с мрежата или производителността. Инструментите за регистриране и наблюдение могат да ви предупредят за проблем, но често нямат достатъчно данни, за да определите основната причина за проблема или степента на заплахата.

Улавянето на пакети попълва основните липсващи подробности, от които се нуждаете, за да разрешите прекъсвания, проблеми с производителността или заплахи за киберсигурността. Използването на улавяне на пакети ускорява процеса на реагиране при инцидент, точно както записите от камери за видеонаблюдение могат да ускорят разследванията на местопрестъплението.

Улавянето на мрежови пакети може да се извърши по различни начини. На най-елементарно ниво пакетите могат да бъдат прихванати и записани с помощта на софтуер за улавяне на пакети, инсталиран на персонален компютър и настройка на мрежова карта (NIC) на „безразборен режим“, за да „слуша“ целия трафик в мрежата. Исторически това често се е наричало „ подслушване на пакети “.

По-усъвършенстваните решения за улавяне на пакети обикновено използват специален хардуер за улавяне на пакети (или виртуални машини в облачни среди) и се наричат по различни начини - мрежови записващи устройства, мрежови снифери, мрежови анализатори, анализатори на пакети или устройства за улавяне на пакети.

И в двата случая решенията за улавяне на пакети получават целия трафик в мрежата, независимо от предназначението му. Всеки пакет, получен на порта за наблюдение, се записва на диск. Други устройства в мрежата не знаят и не се влияят от процеса на улавяне на пакети. Това често се нарича пасивно наблюдение или наблюдение извън обхвата.

Wireshark™ е популярен инструмент за декодер и анализатор на пакети с отворен код, който се инсталира лесно на Windows или MacOS. Той улавя и показва мрежови пакети и е полезен за преглед на малки файлове за улавяне на пакети, експортирани от други системи за улавяне на пакети. Повечето потребители могат да започнат да работят в рамките на няколко минути след инсталирането, да улавят пакети от всеки интерфейс на своя лаптоп и да преглеждат декодирания с помощта на Wireshark GUI. Освен това има няколко хубави вградени инструмента за анализ, които могат да предоставят полезна статистика или да анализират телефонен или безжичен трафик.

2.2 Анализ на протокола

Анализаторът на протоколи е инструмент за измерване или устройство, използвано за улавяне и наблюдение на данни по комуникационен канал. Той улавя данните в комуникационния канал и прикрива битовете данни в смислена протоколна последователност. Анализаторът на протоколи използва комбинация от софтуер и хардуер за анализиране и улавяне на данните по комуникационния канал. Той дава възможност на инженера да разбере протокола и допълнително да анализира уловената последователност от протоколи.

Индустрията има два вида анализатори на протоколи. Анализатор на хардуерен протокол и анализатор на софтуерен протокол.

Анализатор на хардуерен протокол: Анализаторът на хардуерен протокол използва хардуер и софтуер за улавяне на пакетите. Хардуерно базиран анализатор на протоколи се използва за отстраняване на грешки в хардуер и сложни интерфейси на SoC протокол. Хардуерно базираният анализатор на протоколи улавя пакетите от интерфейсите за анализ надолу по веригата. Някои от често срещаните хардуерно базирани анализатори на протоколи са UFS анализатор на протоколи, eMMC анализатор на протоколи, PCIe анализатор на протоколи.

Софтуерен анализатор на протоколи: Софтуерният анализатор на протоколи използва само софтуер за улавяне и анализиране на протокола. Те са известни като мрежови анализатори. Софтуерният протоколен анализатор се използва за улавяне и анализ на LAN, безжична мрежа и др.

2.3 Анализ на трафика

За да се визуализира правилно процесът на мрежовия трафик, той е описан с помощта на модела OSI (модел за взаимно свързване на отворени системи) - абстрактна концептуализация на 7-те слоя на мрежова комуникация, публикувана през 1984 г. от Международната организация по стандартизация (ISO) . Рамката е както следва:

Физически слой: Първият и най-нисък слой се отнася до физическата и електрическата връзка между мрежите. Това може да варира от

електрически вериги и кабели до напрежение и Wi-Fi сигнали – всичко, което действа като непосредствен интерфейс за предаване на необработени данни.

Слой на връзката с данни: Слоят на връзката с данни функционира главно за откриване и коригиране на грешки, направени във физическия слой и за опаковане на байтове данни в рамки за предаване към мрежовия слой и синхронизиране на пакети. Този слой обикновено се разделя на подкатегории на контрол на достъпа до медиите (MAC) и контрол на логическата връзка (LLC) .

Мрежов слой: Третият слой на модела е отговорен за маршрутизирането на пакети с данни от източника до целевия хост през една или повече мрежи. Мрежовият слой задава изисквания за услуги на слоя за връзка за данни и отговаря на заявки за услуги от транспортния слой.

Транспортен слой: Транспортният слой управлява връзките и грешките, за да достави данни до подходящия приложен процес на хост компютъра. Най-известният транспортен протокол на този слой е протоколът за управление на предаването (TCP) .

Слой на сесията: Този слой улеснява диалога между двете устройства, опитващи се да комуникират информация. Услугите на сесийния слой се използват най-вече в настройките на приложението, които използват извиквания на отдалечени процедури (RPC) и предоставят процедури за контролна точка, отлагане, прекратяване и рестартиране.

Презентационен слой: Презентационният слой гарантира, че данните, препредадени към приложния слой, са лесни за четене и достъпни. Дешифрирането и криптирането се случват най-вече тук – което прави този слой необходим за преобразуването на данни в по-„представително“ предаване.

Слой на приложението: Последният слой на мрежовия модел е този, който е най-близък до потребителския изход – предоставяйки на потребителите директен интерфейс и форма на достъп до мрежата на този слой. Услугите, които разчитат на приложния слой, включват TelNet , FTP и ежедневни уеб браузъри.

Анализът на мрежовия трафик (NTA) е метод за наблюдение на наличността и активността на мрежата за идентифициране на аномалии, включително проблеми със сигурността и работата. Обичайните случаи на използване на NTA включват:

- Събиране в реално време и исторически запис на това, което се случва във вашата мрежа
- Откриване на злонамерен софтуер , като например ransomware активност
- Откриване на използването на уязвими протоколи и шифри
- Отстраняване на неизправности при бавна мрежа
- Подобряване на вътрешната видимост и премахване на слепите петна

Анализът на мрежовия трафик (NTA) е усъвършенстван метод за проверка и разбивка на пакетите с данни, които го формират, чрез използване на

комбинация от моделиране на поведението, машинно обучение и базирано на правила откриване за изкореняване на всяка подозрителна дейност. Базовата линия на нормалното поведение може да бъде идентифицирана чрез този анализ и всички отклонения могат да бъдат маркирани и изолирани като потенциални заплахи.

Докато това се използва най-вече за целите на сигурността, анализът на мрежовия трафик може да се използва и за планиране на капацитета и идентифициране на пикове на мрежовия трафик в определени области.

2.4 Анализ на производителността

Ефективността на мрежата е "анализът и прегледът на колективната мрежова статистика, за да се определи качеството на услугите, предлагани от основната компютърна мрежа [което е] основно измерено от гледна точка на крайния потребител."

По-просто, производителността на мрежата се отнася до анализ и преглед на производителността на мрежата, както се вижда от крайните потребители.

Както бе споменато по-горе, за да наблюдаваме производителността от гледна точка на потребителя, трябва да извършим тестове за производителност на мрежата от същата гледна точка.

В идеалния случай за да направите това, вие искате да наблюдавате производителността на мрежата от местоположението на крайния потребител, без да се налага да инсталирате инструмент за мрежово измерване на всяка потребителска работна станция.

Освен това не искате да улавяте всеки пакет данни за анализ, което ще изисква много допълнителен хардуер и може да наруши поверителността на вашия потребител.

Когато искате да измерите мрежови показатели, производителност и история, можете да използвате временни инструменти като traceroutes и ping, за да идентифицирате проблеми. Това може да ви даде представа за текущите проблеми, но ако искате да отстраните периодични проблеми с мрежата, не можете да използвате временни инструменти.

За това можете да използвате софтуер който да симулира гледната точка на потребителят като непрекъснато наблюдение на производителността, използвайки синтетичен трафик. Те също:

- Измерват мрежови показатели като трептене, загуба на пакети, пропускателна способност и други
- Периодични мрежови проблеми, които е трудно да се определят
- Предупреждава за всяко влошаване на производителността
- Събиране на данни, за да помогнете за отстраняване на неизправности

2.5 Анализ на сигурността

Компютърна мрежа се отнася до няколко компютри, които са свързани към основен сървър, от който компютрите могат да споделят и обменят информация и програми. Анализът на мрежовата сигурност е акт на наблюдение на мрежа за пропуски, които могат да позволят на хора извън мрежата да преглеждат или прихващат потенциално чувствителна

информация. Има редица фактори, които се вземат предвид от професионалист или специалист, който анализира сигурността на мрежата.

Анализът на мрежовата сигурност може да започне с оторизацията или удостоверяването на потребители в мрежата. Това най-често се постига, като се изисква от потребителя да въведе име и парола, за да влезе. Тъй като тази информация понякога може да бъде позната или открадната от потенциални мрежови нарушители, анализаторът често ще проверява за фактори като сложността на паролата. В по-напредналите системи удостоверяването може да се провери чрез използване на пръстов отпечатък или гласово разпознаване.

След това анализът на мрежовата сигурност трябва да включва тестване на защитната стена на мрежата. Защитната стена е компонент на мрежовата сигурност, който е отговорен за ограничаването на достъпа на определени потребители до определени видове привилегирована информация. Докато този компонент е ефективен при ограничаване на достъпа на тези, на които вече е разрешено да влизат в мрежа, важно е да се разбере, че защитната стена не може да сканира за вируси, червеи или зловреден софтуер, които са предназначени да причинят вредни неизправности в мрежите .

Поради тази причина анализът на мрежовата сигурност трябва да включва и тестване на сканиране за вируси. Това са компоненти, които са предназначени да проверяват всички видове входящи данни за потенциално опасни елементи. Тъй като червеите, вирусите и зловреден софтуер често се развиват или еволюират бързо, важен аспект от анализа на мрежовата сигурност е актуализирането на програмите за сканиране на вируси. Това е процес, при който анализаторът се уверява, че антивирусният софтуер е в

състояние да открие най-актуалните видове зловреден софтуер, който може да зарази мрежата.

3 Обстойно разглеждане на мрежов дизайн за най-добра производителност.

Преди да започнете да проектирате вашата LAN, трябва да определите вашите нужди и цели за вашата мрежа. Какви са основните функции и приложения на вашата LAN? Колко потребители и устройства ще имат достъп до мрежата? Какви са очакваните модели на трафик и изисквания за честотна лента? От колко мащабируемост и гъвкавост се нуждаете? Как ще гарантирате сигурността и поверителността на вашите данни? Тези въпроси ще ви помогнат да определите обхвата, размера и структурата на вашата локална мрежа, както и хардуерните и софтуерните компоненти, от които ще се нуждаете.

Топологията и архитектурата на вашата LAN се отнасят до физическото и логическото оформление на вашите мрежови устройства и връзки. Съществуват различни типове топологии и архитектури, като шина, пръстен, звезда, мрежа, йерархична, peer-to-peer и клиент-сървър. Всеки от тях има своите предимства и недостатъци, в зависимост от вашите нужди и цели. Например звездообразната топология е проста и лесна за управление, но изисква централно устройство, като превключвател или хъб, което може да се превърне в единична точка на отказ. Мрежестата топология е устойчива, но изисква повече кабели и устройства, което може да увеличи разходите и сложността. Трябва да изберете топологията и архитектурата, които най-добре отговарят на размера, производителността, надеждността и сигурността на вашата локална мрежа.

Устройствата и технологиите, които използвате за вашата локална мрежа, ще повлияят на нейната функционалност и ефективност. Ще трябва да изберете подходящите устройства и технологии за вашия мрежов слой, слой за връзка с данни и физически слой. Например на мрежовия слой ще трябва да решите дали да използвате рутер, защитна стена или и двете, за да свържете вашата LAN към други мрежи и да я защитите от външни заплахи. На слоя за връзка за данни ще трябва да решите дали да използвате комутатор, хъб или и двете, за да свържете вашите мрежови устройства и да контролирате потока от данни. На физическия слой ще трябва да решите дали да използвате кабелни или безжични технологии, като Ethernet, Wi-Fi или оптични влакна, за предаване на данни по кабели или ефирни вълни. Трябва да изберете устройствата и технологиите, които отговарят на стандартите за производителност, сигурност и съвместимост на вашата локална мрежа.

Мрежовото сегментиране и адресиране са техники, които могат да ви помогнат да организирате и управлявате вашата LAN по-ефективно. Сегментирането на мрежата е процесът на разделяне на вашата локална мрежа на по-малки подмрежи или подмрежи въз основа на логически критерии, като функция, местоположение или отдел. Мрежовото адресиране е процес на присвояване на уникални идентификатори или адреси на всяко устройство и подмрежа във вашата LAN. Мрежовото сегментиране и адресиране може да ви помогне да подобрите производителността, сигурността и мащабируемостта на вашата LAN. Например, чрез създаване на подмрежи можете да намалите претоварването на мрежата, да изолирате мрежовите проблеми и да наложите политики за достъп. Като използвате адреси, можете да

идентифицирате и локализирате мрежови устройства, както и да насочвате данни към правилната дестинация.

Мрежовите стандарти и протоколи са правила и конвенции, които управляват как мрежовите устройства комуникират и взаимодействат едно с друго. Следването на мрежови стандарти и протоколи може да ви помогне да осигурите оперативна съвместимост, съвместимост и качество на вашата LAN. Има различни видове мрежови стандарти и протоколи, като IEEE, TCP/IP, DHCP, DNS и SNMP. Всеки от тях дефинира специфични аспекти на мрежовата комуникация, като формат на данните, метод на предаване, схема за адресиране, процес на конфигуриране или функция за управление. Трябва да следвате мрежовите стандарти и протоколи, които са подходящи и приложими за устройствата, технологиите и функциите на вашата LAN.